Utilizing Snort in the Analysis of Intrusion Detection System

This thesis is presented to the Graduate School
in fulfillment of the requirements for
Master of Science (Information Technology)
Universiti Utara Malaysia

By
Noorulsadiqin Azbiya binti Yaacob

SEKOLAH SISWAZAH
(GRADUATE SCHOOL)
UNIVERSITI UTARA MALAYSIA

PERAKUAN KERJA / TESIS
(Certification of Thesis Work)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

NOORULSADIQIN AZBIYA YAACOB

calon untuk Ijazah
(candidate for the degree of) **SARJANA SAINS (TEKNOLOGI MAKLUMAT)**

telah mengemukakan tesis/disertasinya yang bertajuk
(has presented his/her thesis work of the following title)

UTILIZING SNORT IN THE ANALYSIS OF INTRUSION DETECTION SYSTEM

seperti yang tercatat di muka surat tajuk dan kulit tesis/disertasi
(as it appears on the title page and front cover of thesis work)

bahasa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan, dan liputan bidang ilmu yang memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada :
(that the thesis/dissertation is acceptable in form and content, and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate through an oral examination held on **21 OGOS 2003**

Pengerusi Viva *(Chairman for Viva)*	:Prof. Dr. Ku Ruhana Ku Mahamud	Tandatangan: *(Signature)*
Penilai Luar *(External Assessor)*	:Dr. Azman Samsudin	Tandatangan: *(Signature)*
Penilai Dalaman *(Internal Assessor)*	:En. Azmi Md Saman	Tandatangan: *(Signature)*
Penyelia Utama *(Principal Supervisor)*	:En. Hatim Mohd. Tahir	Tandatangan: *(Signature)*
Dekan Sekolah Siswazah *(Dean Graduate School)*	:Prof. Dr. Juhary Hj. Ali	Tandatangan: *(Signature)*

Tarikh
(Date) : **21 OGOS 2003**

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for a Master of Science in Information Technology degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in his absence, by the Dean of Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 Sintok, Kedah

ABSTRAK

Matlamat penyelidikan ini adalah untuk merekabentuk satu set penilaian sistem pengesanan pencerobohan. Set ini dibina berdasarkan kepada empat keperluan asas sistem pengesanan pencerobohan yang dinyatakan oleh Porras dan Valdes (1998) dan Debar et al (1999) iaitu kejituan, prestasi, kesempurnaan dan toleransi kegagalan. Set pengujian yang telah dibina diuji dengan menggunakan satu sistem pengesanan pencerobohan terbuka iaitu Snort. Metodologi dan prosedur pengujian yang digunakan semasa penilaian ke atas sistem pengesanan pencerobohan adalah berdasarkan kepada model simulasi. Hasil daripada pengujian menggunakan set penilaian yang dibentuk, didapati ia dapat mendedahkan kelemahan sesuatu sistem pengesanan pencerobohan. Kelemahan yang dikesan boleh digunakan untuk meningkatkan lagi keupayaan sistem pengesanan pencerobohan dari semasa ke semasa.

ABSTRACT

The objective of this research is primarily to construct a set of intrusion detection system evaluation. The set is built through four basic needs of intrusion detection as stated by Porras and Valdes (1998) and Debar et al (1999) which comprise of accuracy, performance, completeness and fault tolerance. The test set built is then tested by using open intrusion detection system, Snort. The methodology and the testing procedure which are used during the evaluation of intrusion detection system is based on a simulation model. Results from the evaluation set consrtucted is found able to expose any existing weaknesses in the intrusion detection system. Any weaknesses detected will then be used to upgrade the intrusion detection system from time to time.

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful,

I would like to thank:

The Ministry of Science and Technology for the financial support,

The Universiti Utara Malaysia for the facilities and resources provided,

The ex-dean, Proffesor Dr. Abu Talib Othman for being the first one to grab my attention to field of research study,

My supervisor, Encik Hatim Mohamad Tahir for his help with writing papers, attending conferences, resolving technical matters and developing the thesis during the course of my master,

My dear friend, Ahmad Hanis Mohd Shabli for his enthusiastic support, tireless effort and constant patience when dealing with my bugs, queries and general ramblings,

My meticulous proof reader, Syed Zami Zaffaran for checking my English and re-reading the thesis,

My other friends and colleagues in the lab, both past and present, who have help me along the way,

My close friends and family, whose constant love and support give me confidence in all aspects of life.

✧

I would like to dedicate this thesis to my adorable friend and my parents who lovingly encouraged and supported me throughout this research. The motivation for all I do.

✧

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ASCII	=	American Standard Code For Information Interchange
CGI	=	Common Gateway Interface
CIDR	=	Classless Inter-Domain Routing
CORBA	=	Common Object Request Broker Architecture
DMZ	=	DeMilitarized Zone
DNS	=	Domain name system
FTP	=	File Transfer Protocol
HIDS	=	Host-based Intrusion Detection System
HIDSs	=	Host-based Intrusion Detection Systems
HTTP	=	HyperText Transfer Protocol
ICMP	=	Internet Control Message Protocol
ID	=	Intrusion Detection
IDES	=	Intrusion Detection Expert System
IDS	=	Intrusion Detection System
IP	=	Internet Protocol
LAN	=	Local Area Network
LANL's	=	Los Alamos National Laboratorary's
LARIAT	=	Lincoln adaptable real-time information assurance test bed
MIDAS	=	Multics Intrusion Detection and Alerting System
NADIR	=	Network Anomaly Detection and Intrusion Reporter
NFR	=	Network Flight Recoder
NIDES	=	Next-Generation Intrusion-Detection Expert System
NIDS	=	Network-based Intrusion Detection System
NIDSs	=	Network-based Intrusion Detection Systems
NT SAM	=	Windows NT Security Accounts Manager
OS	=	Operating System
PBX	=	Private Branch Exchange
POP	=	Post Office Protocol
SMB	=	Server Message Block
SMTP	=	Simple Mail Transfer Protocol
SQL	=	Server Query Language

SRI	=	Stanford Research Institute
SSH	=	Secure shell
SSO	=	Site Security Officer
TCP/IP	=	Transmission Control Protocol/Internet Protocol
TCP/UDP	=	Transmission Control Protocol/User Datagram Protocol
USTAT	=	UC Santa Barbara's State Transition Analysis Tool

CHAPTER 1
INTRODUCTION

Nowadays the En of Internet technology itself can in turn be manipulated to the attacker's whim-who is always on the prowl to infiltrate any given network. This situation brings about a high demand for computer system's security, which includes the computer's network to ensure safety. Precisely, network security is important to protect confidentiality, integrity and availability of data or information that passed through or existed in any computer's system or its network.

Computer system for most organization usually links all existing computers through a network. Its design is such that it allows users to access any computers in an organization's computer system to get information and data. For a much bigger computer network, it can also be directly linked to the Internet network. Therefore, the network faces a much bigger risk of attack. Furthermore, up to now there is no mechanism that can promise to entirely secure a network. Among the available security methods for network's protection are encryption, access control and authentication of users, authentication of distributed systems, traffic control and data integrity.

Encryption is a means to send information in a form that is 'unreadable'. When the information arrives at its destination, it can be reconfigured so that the receiver can read it. There are two types of encryption: link encryption and end-to-end encryption. Link encryption is the data security process of encrypting information at the data link level as it is transmitted between two points within a network. Data which is plaintext in the host server, is encrypted when it leaves the host, decrypted at the next link (which may be a host or a relay point) and then re-encrypted before it continues to the next link. The process is repeated until the data has reached the recipient. While end-to-end encryption is the encryption of information at its origin and decryption at its intended destination without any intermediate decryption.

The contents of the thesis is for internal user only

REFERENCES

Ahuja, V. (1996). Network and Internet Security. United States of America: AP Professional.

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E. (2000). State of The Practice of Intrusion Detection Technologies. (Tech. Rep. CMU/SEI-99-TR-028). Carnegie Mellon University, Software Engineering Institute.

Allessandri, D. (2000). Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems. (Tech. Rep. rz3225). IBM Research, Zurich Research Laboratory.

Amoroso, E. (1999). Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books.

Anderson, J. (1980). Computer Security Threat Monitoring and Surveillance. (Tech. Rep.). Fort Washington, Pennsylvania: James P. Anderson Company.

Anderson, D., Frivold, T., and Valdes, A.(1995). Next-generation intrusion detection expert system (NIDES). (Tech. Rep. SRI-CSL-95-07). Menlo Park, California : SRI International, Computer Science Laboratory.

Asaka, M., Okazawa, S., Taguchi, A., and Goto, S. (1999). A Method of Tracing Intruders by Use of Mobile Agents. Proceedings of the 9th Annual Conference of the Internet Society (INET'99).

Axelsson, S. (1999). On a Difficulty of Intrusion Detection. Web proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99), http://www.Raid-symposium.org/raid99.

Bace, R.(1999). An Introduction to Intrusion Detection Assessment. http://ca.com./solutions/enterprise/etrust/intrusion_detection/product_info/intrusion_assess.pdf.

Bace, R., and Mell, P. (2001). NIST Special Publication on Intrusion Detection Systems. NIST (National Institute of Standards and Technology) Special Publication 800-31.

Balasubramanian, S. (2000). An Architecture for Protection of Network Hosts from Denial of Service Attacks. Master's Thesis. University of Florida.

Borgwardt, M. (1999). Testing Intrusion Detection Systems: Methods and Tools. Paper presented at Experimental Methods in Software Engineering Seminar. Technische Universitat Munchen.

Carter, E. (2002). Cisco Secure Intrusion Detection System. United States of America: Cisco Systems, Inc.

Crosbie, M. and Price, K. (1999). COAST Intrusion Detection System, COAST Laboratory, Purdue University, http://www.cerias.purdue.edu/coast/intrusion-detection/ids.html.

Debar, H., Dacier , M., Wespi, A. (1999). Towards A Taxonomy of Intrusion-Detection System. Computer Network, 31, 805-822.

Debar, H., Dacier , M., Wespi, A., Lampart, S. (1999). An Experimental Workbench for Intrusion Detection Systems. (Research Report RZ 2998). IBM Research Division, Zurich Research Laboratory.

Denning, D. (1987). An Intrusion-Detection Model. IEEE transaction on Software Engineering, 13(2), 222-223.

Durst, R., Champion, T., Witten, B., Miller, E., and Spagnuolo, L. (1999). Testing and Evaluating Computer Intrusion Detection Systems. Communications of the ACM. 42(7), 53-61.

Fyodor, Y. (2000). 'Snortnet' - A Distributed Intrusion Detection System. IVT-1/95, Kyrgyz Russian Slavic University,Bishek, Kyrgyzstan.

Jansen, W., Mell, P., Karygiannis, T., and Marks, D. (2000). Mobile Agents in Intrusion Detection and Response. In Proceedings of the 12th Annual Canadian Information Technology Security Symposium.

Kanlayasiri, U., Sanguanpong, S., and Jaratmanachot W. (2000). A Rule-based Approach for Port Scanning Detection. In Proceedings of the 23rd Electrical Engineering Conference, Chiang Mai Thailand.

Krugel, C. and Toth, T. (2000). A Survey on Intrusion Detection Systems. (Tech. Rep. TUV-1841-00-11). Technical University of Vienna, Distributed Systems Group.

Levitt, K. and Bishop, M. (1996). Misuse Detection Research Study. Reader's Digest Condensed Version. Department of Computer Science, University of California.

Lippman, R., Haines, J.W., Fried D.J., Graf, I., Kendall, K.R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K, and Zissman, M.A. (1999). Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation. IEEE.

Lippman, R., Haines, J.W., Fried D.J., Korba, J., and Jas, K. (2000). Analysis and Results of the 1999 DARPA Off-line Intrusion Detection Evaluation. In Debar, H., Me, L., and Wu, S.F., editors.

Lippman, R., Haines, J.W., Fried D.J., Korba, J., and Jas, K. (2000). The 1999 DARPA Off-Line Intrusion Detection Evaluation. Computer Networks, 34(4), 579-595.

Long, L., and Long, N. (1993). Computers. United States of America: Prentice-Hall, Inc.

McHugh, J. (2000). The Lincoln Laboratory Intrusion Detection Evaluation: A Critique. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition.

Mukherjee, B., Heberlein, L., and Levitt, K. (1994). Network Intrusion Detection. IEEE Network, 8(3), 26-41.

Myers, G.J. (1979). The Art of Software Testing. United States of America: John Wiley & Sons, Inc.

Northcutt, S. and Novak, J. (2001). Network Intrusion Detection An Analyst's Handbook. (Second Edition). United States of America: New Riders.

Perry, W. (1995). Effective Methods for Software Testing. United States of America: John Wiley & Sons, Inc.

Porras, P.A. and Valdes, A. (1998). Live Traffic Analysis of TCP/IP Gateways. In Proceedings of the 1998 ISOC Symposium on Network and Distributed System Security (NDSS'98).

Price, K. (1999). Purdue University Intrusion Detection Pages. Http://www.cerias.purdue.edu/coast/intrusion-detection/.

Puketza, N.,Chung, M., Olsson, R., and Mukherjee, B. (1997). A Software Platform for Testing Intrusion Detection Systems. IEEE Software, 14(5), 43-51.

Puketza, N.F., Zhang, K., Chung, M., Mukherjee, B., and Olsson, R.A. (1996). A Methodology for Testing Intrusion Detection Systems. IEEE Tansactions on Software Engineering, 22, 719-729.

Ranum, M.J. (2000). Intrusion Detection and Network Forensic. M1 Tutorial – USENIX Security 2000, Denver, Colorado, USA.

Ranum, M.J. (2001). IDS Benchmarking Experiences Benchmarking Intrusion Detection Systems. NFR Security Technical Publications.

Roesch, M. (1999). Snort – Lightweight Intrusion Detection System for Networks. In Proceedings of the USENIX LISA'99 conference.

Rossey, L.M., Cunningham, R.K., Fried, D.J., Rabek, J.C., Lippmann, R.P., and Haines, J.W. (2001). LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed. Paper presented at Fourth International Workshop on Recent Advances in Intrusion Detection (RAID2000).

Shipley, G., and Mueller, P. (2001). To Catch a Thief. Network Computing. 37-62. www.networkcomputing.com.

Shipley, G., and Mueller, P. (2001). Dragon Claws its Way to the Top. Network Computing. www.networkcomputing.com.

Spafford, E., and Zamboni, D. (1998). AAFID: Autonomous Agents for Intrusion Detection. Web Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). http://www.raid-symposium.org/raid98.

Sundaram, A. (2001). An introduction to intrusion detection. The ACM Crossroads Student Magazine. http://www.acm.org/crossroads/xrds2-4/intrus.html.

Turban, E. and Aronsson, J.E. (1998). Decission Support Systems and Intelligent Systems. (International Edition). Upper Saddle River, N.J: Prentice Hall.

Wan, T. and Yang X. (2001). IntruDetector: A Software Platform for Testing Network Intrusion Detection Algorithms. Paper presented at 17th Annual Computer Security Applications Conference (ACSAC'01).